BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Ketika teknologi terus berkembang, perlunya keamanan pesan dalam komunikasi modern juga semakin mendesak. Risiko pencurian data dan serangan siber semakin meningkat, membuat perlindungan terhadap pesan menjadi lebih krusial. Pesan teks yang dikirim bisa terganggu oleh pihak tidak bertanggung jawab yang ingin mengetahui isi percakapan karena kurangnya proses enkripsi.

Kriptografi merupakan teknik untuk menjaga kerahasiaan pesan. Dalam ilmu kriptografi, teks asli pesan (*plaintext*) diubah menjadi teks terenkripsi (*ciphertext*) melalui penggunaan sebuah kunci enkripsi. Tahapan ini menyulitkan pembacaan pesan oleh individu yang tidak memiliki kunci dekripsi yang tepat (Putri et al., 2019). Kriptografi klasik merupakan metode pengamanan pesan yang telah digunakan selama berabad-abad. Dalam bidang Kriptografi klasik memanfaatkan metode enkripsi simetris di mana satu kunci digunakan untuk melaksanakan proses enkripsi dan dekripsi (Amin, 2017). Pengetahuan tentang kriptografi juga berperan sebagai metode untuk menjaga keamanan data. bisa dicapai dengan metode yang beragam, termasuk di dalamnya adalah dengan memanfaatkan pendekatan enkripsi *caesar*.

Enkripsi adalah salah satu cabang di dalam domain kriptografi adalah teknik enkripsi. Tujuan utama dari proses enkripsi adalah mengubah teks menjadi formulasi yang rumit dan sukar dimengerti, sehingga kontennya menjadi kabur dan kurang jelas dalam pemahaman. Dalam enkripsi, terdapat dua metode utama yang digunakan, yaitu metode kunci simetris dan metode

kunci asimetris. Ada beberapa algoritma yang dapat digunakan untuk melakukan enkripsi menggunakan kunci simetris. Tiga contohnya termasuk *Caesar Cipher*, *Vigenere Cipher*, dan *Affine Cipher* (Hardita & Sholeha, 2021).

Caesar cipher, yang juga dikenal sebagai sandi *caesar*, merupakan sebuah metode kriptografi klasik yang mengandalkan penggantian sederhana. Prosedur enkripsi dan dekripsi dalam sandi *caesar* dilakukan melalui pergeseran, yang menggantikan suatu huruf dengan huruf pada abjad dengan jarak -k atau +k dari huruf tersebut (Hardita & Sholeha, 2021). *Cipher caesar* adalah varian dari sandi substitusi yang membentuk sebuah sandi di mana masing-masing huruf digantikan oleh huruf yang terletak beberapa langkah tertentu di dalam abjad dalam pesan digeser sejumlah langkah tertentu dalam alfabet (Putri et al., 2019).

Pada metode algoritma *caesar cipher*, tiap karakter pada pesan asli (*plaintext*) diubah menjadi karakter lain dalam urutan alfabet dengan pergeseran posisi yang khusus. Pergeseran ini dilakukan untuk setiap karakter dalam pesan dan disesuaikan dengan kunci yang telah ditentukan (Fatonah et al., 2019). Sebagai contoh, jika nilai kunci adalah n = 3, setiap abjad akan maju tiga langkah, sehingga huruf A menjadi huruf D, gantikan huruf B dengan huruf E, dan lakukan substitusi serupa untuk huruf-huruf berikutnya sesuai dengan pergeseran tersebut. Metode *caesar cipher* juga memiliki peran penting sebagai dasar pemahaman dalam bidang kriptografi sebelum mempelajari metode kriptografi yang lebih kompleks berbasis karakter.

Seperti pada penelitian (Sari et al., 2022) Penerapan metode dalam penelitian ini berfokus pada cara kerja kriptografi dan cara melindungi informasi teks yang tersimpan dalam basis data akan aman dari entitas yang

tidak memiliki izin. Aplikasi kriptografi ini bertujuan untuk menjaga kerahasiaan informasi tentang produk, penyedia, konsumen, dan rincian transaksi, serta mencegah penyebaran oleh pihak yang tidak dapat dipertanggungjawabkan, berdasarkan pelaksanaan dan percobaan program, PT. Multi Mitra Usaha Bersama telah berhasil menjaga dan melindungi kerahasiaan informasi dengan sukses. Keberhasilan ini memberikan keunggulan kepada perusahaan dalam menjalankan tugas-tugas inti, fungsi, serta perannya dalam memastikan keamanan teknologi.

Keamanan dan privasi informasi adalah elemen yang signifikan dalam komunikasi melalui komputer. Sehingga, studi ini berfokus pada penggunaan teknik kriptografi sandi *caesar* untuk memastikan perlindungan teks pendek dengan efektif. Dan mendapati permasalahan yang disebutkan di atas, peneliti merasa memiliki ketertarikan untuk menjalankan penelitian yang diberi judul "IMPLEMENTASI KRIPTOGRAFI DENGAN MENGGUNAKAN METODE CAESAR CIPHER UNTUK KEAMANAN FILE DAN TEKS SINGKAT" dimana pada penelitian ini, diharapkan meningkatkan keamanan karena dengan mengenkripsi teks singkat sebelum dikirim ke server, potensi serangan pada informasi sensitif dapat dikurangi.

1.2 RUMUSAN MASALAH

1) Bagaimana cara untuk melaksanakan pengamanan teks singkat menggunakan kriptografi klasik?
2) Bagaimana cara mengimplementasikan pengamanan teks menggunakan kriptografi *caesar cipher*?
3) Bagaimana cara mengelola kunci enkripsi untuk dokumen?

1.3 BATASAN MASALAH

Agar tidak meyebabkan salah presepsi dan luasnya pokok pembahasan, maka diterapkan batasan-batasan sebagai berikut:

1) Informasi yang disisipkan berupa file *text* dan metode yang diambil adalah *caesar cipher*.
2) Objek penelitian difokuskan pada pengamanan teks singkat dengan menggunakan metode *caesar cipher*.
3) Pengamanan data untuk dokumen (*pdf,dox*).

1.4 TUJUAN PENELITIAN

1) Mengetahui cara meningkatkan keamanan pada teks singkat menggunakan kriptografi klasik.
2) Menguji keamanan teks menggunakan metode *caesar cipher*.
3) Mengamankan data berbentuk dokumen yang berisi file *text*.

1.5 MANFAAT PENELITIAN

1) Dengan menggunakan metode *caesar cipher*, dapat memberikan tingkat keamanan yang lebih baik pada saat pengguna mengirim pesan yang berupa informasi.
2) Dapat meningkatkan privasi keamanan bagi pengguna agar pengguna merasa lebih aman.